PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

CUMPLIMIENTO CT-CUM/A-47-2023
Derivado de los expedientes CT-CI/A-27-2018 y CT-CUM-R/A-2-2019

INSTANCIA VINCULADA:

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente al ocho de noviembre de dos mil veintitrés.

A N T E C E D E N T E S:

PRIMERO. I. Solicitud de información. El veinticuatro de septiembre de dos mil dieciocho, se recibió en la Plataforma Nacional de Transparencia la solicitud tramitada con el folio 0330000178918, en la que, una vez desahogada la prevención, se señaló:

> *"En atención a su requerimiento preciso que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, la información pública solicitada es la siguiente:*
> *1. Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero:*
>
> *a) Si actualmente los archivos electrónicos almacenados en la unidad de disco duro (que no sean del sistema operativo) cuentan con algún tipo de cifrado, cuyo control se efectué por medio de contraseñas o credenciales administrativas.*
> *b) Nombres comerciales de los programas informáticos utilizados para el cifrado de los archivos mencionados en el inciso anterior.*
> *c) Si actualmente los usuarios del equipo pueden borrar los archivos electrónicos almacenados en la unidad de disco duro (que no sean del sistema operativo), sin la necesidad de contar con privilegios o contraseñas administrativas.*
> *d) Si se encuentra instalado el navegador de Internet denominado Tor Browser.*
> *e) Número de puertos USB (por sus siglas en ingles Universal Serial Bus) habilitados para su funcionamiento.*

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

f) Si actualmente los usuarios del equipo pueden copiar los archivos almacenados en la unidad de disco duro (que no sean del sistema operativo) a través de los puertos USB mencionados en el punto anterior, sin la necesidad de contar con privilegios o contraseñas administrativas.

NOTA: Se reitera me entregue la información a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar,"

SEGUNDO. Resolución del Comité de Transparencia en que se reservó información. En sesión de treinta y uno de octubre de dos mil dieciocho, se emitió resolución en el expediente CT-CI/A-27/2018[1], la cual se transcribe en lo conducente:

II. Materia de análisis. *Como se aprecia del antecedente I, en la solicitud se pide que a partir del número de serie de cada uno de los equipos de cómputo en posesión de la Suprema Corte de Justicia de la Nación, se informe lo siguiente:*

a) Si los archivos almacenados en el disco duro cuentan con algún tipo de cifrado, cuyo control se efectúe por contraseñas o credenciales administrativas.
b) Nombres comerciales de los programas informáticos utilizados para el cifrado.
c) Si los usuarios de los equipos pueden borrar los archivos almacenados en el disco duro, sin la necesidad de contar con privilegios o contraseñas administrativas.
d) Si se encuentra instalado el navegador de Internet denominado 'Tor Browser'.
e) Número de puertos 'USB' habilitados para su funcionamiento.
f) Si los usuarios de los equipos pueden copiar los archivos almacenados en el disco duro, a través de los puertos 'USB', sin la necesidad de contar con privilegios o contraseñas administrativas.

Conforme al informe transcrito en el antecedente VI, se tiene por atendido lo requerido en el inciso d), en virtud de que la Dirección General de Tecnologías de la Información informó que los equipos que proporciona de forma predeterminada llevan enlistados los navegadores 'Microsoft Edge y Microsoft Internet Explorer', pero el navegador 'Tor Browser' no se encuentra listado; por tanto, la Unidad General de Transparencia deberá hacer del conocimiento peticionario dicha respuesta y ello no será materia de análisis en la presente resolución.

III. Análisis. Información reservada.

[1] Disponible en: https://www.supremacorte.gob.mx/sites/default/files/resoluciones/2019-01/CT-CI-A-27-2018.pdf

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

Por cuanto a lo requerido en los incisos a), b), c), e) y f) de la solicitud, la Dirección General de Tecnologías de la Información informó que la divulgación de esa información podría comprometer, en distintos aspectos, la seguridad informática de este Alto Tribunal, de ahí que clasifica la información como reservada en términos del artículo 113, fracción I de la Ley General de Transparencia y con apoyo en lo resuelto por este Comité en el expediente CT-CI/A-3-2018.

Sobre esa base, el punto a dilucidar a través del caso que nos ocupa radica en si sobre la información solicitada se actualiza o no la reserva identificada por la instancia requerida y, en su caso, si aquella puede o no ser proporcionada en los términos solicitados.

Antes de llevar a cabo el análisis correspondiente, es importante recordar que en el esquema de nuestro sistema constitucional, el derecho de acceso a la información encuentra cimiento a partir de lo dispuesto en el artículo 6º, apartado A, de la Constitución, cuyo contenido deja claro que, en principio, todo acto de autoridad (todo acto de gobierno) es de interés general y, por ende, es susceptible de ser conocido por todos.

Sin embargo, como lo ha interpretado el Pleno del Alto Tribunal en diversas ocasiones, el derecho de acceso a la información no puede caracterizarse como uno de contenido absoluto, en tanto su ejercicio se encuentra acotado en función de ciertas causas e intereses relevantes, así como frente al necesario tránsito de las vías adecuadas para ello[2].

Así, precisamente en atención al dispositivo constitucional antes referido, se obtiene que la información que tienen bajo su resguardo los sujetos obligados del Estado encuentra como excepción aquella que sea temporalmente reservada o confidencial en los términos establecidos por el legislador federal o local, cuando de su propagación pueda derivarse perjuicio por causa de interés público y seguridad nacional.

Trasladado al caso, como se vio en el apartado de antecedentes, para sustentar la reserva, el área manifestó expresamente que divulgar lo solicitado pondría en riesgo la seguridad informática de la institución por lo siguiente:

---

[2] Corresponde al pie de página número 1 del documento original.
*‘**DERECHO A LA INFORMACIÓN. SU EJERCICIO SE ENCUENTRA LIMITADO TANTO POR LOS INTERESES NACIONALES Y DE LA SOCIEDAD, COMO POR LOS DERECHOS DE TERCEROS**. El derecho a la información consagrado en la última parte del artículo 6o. de la Constitución Federal no es absoluto, sino que, como toda garantía, se halla sujeto a limitaciones o excepciones que se sustentan, fundamentalmente, en la protección de la seguridad nacional y en el respeto tanto a los intereses de la sociedad como a los derechos de los gobernados, limitaciones que, incluso, han dado origen a la figura jurídica del secreto de información que se conoce en la doctrina como ‘reserva de información’ o ‘secreto burocrático’. En estas condiciones, al encontrarse obligado el Estado, como sujeto pasivo de la citada garantía, a velar por dichos intereses, con apego a las normas constitucionales y legales, el mencionado derecho no puede ser garantizado indiscriminadamente, sino que el respeto a su ejercicio encuentra excepciones que lo regulan y a su vez lo garantizan, en atención a la materia a que se refiera; así, en cuanto a la seguridad nacional, se tienen normas que, por un lado, restringen el acceso a la información en esta materia, en razón de que su conocimiento público puede generar daños a los intereses nacionales y, por el otro, sancionan la inobservancia de esa reserva; por lo que hace al interés social, se cuenta con normas que tienden a proteger la averiguación de los delitos, la salud y la moral públicas, mientras que por lo que respecta a la protección de la persona existen normas que protegen el derecho a la vida o a la privacidad de los gobernados. Época: Novena Época. Registro: 191967. Instancia: Pleno. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XI, Abril de 2000. Materia(s): Constitucional*
Tesis: P. LX/2000. Página: 74)’

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

- *Para garantizar la confiabilidad de un documento electrónico se hace uso de 'Algoritmos o métodos de cifrado', los cuales se encargan de transformar el contenido del documento en un conjunto de caracteres sin orden o significado, con la finalidad de que la persona que tenga la llave o clave de acceso puede tener acceso al equipo y a la información contenida en el equipo.*
- *Para realizar el cifrado de un documento se pueden realizar diversos métodos de cifrado, lo que puede ser un procedimiento sencillo, o bien, el uso de algoritmos científicos y comerciales, para lo cual se realiza una gran cantidad de procesos de cómputo.*
- *Cuando se da a conocer el cifrado, se da a conocer el proceso de cifrado del documento, lo que permite, en su caso, acceder a la información de manera sencilla.*
- *Revelar el método de cifrado de cualquier documento, como puede ser comunicaciones, equipos de seguridad, cifrado de correo o cifrado de documentos, permitiría dar a conocer la técnica para proteger la información procesada en esos elementos de cómputo, lo que facilitaría un ataque para la obtención de información.*

En dicho oficio, se agrega que de la información requerida en los incisos a), b), c), e) y f), se podrían presentar algunos riesgos, a saber:

- *Informar los archivos almacenados en disco duro con algún cifrado y que son controlados por contraseña, así como indicar que los usuarios no pueden copiar ni borrar archivos sin necesidad de contar con privilegios o contraseñas, lo que pone en riesgo la integridad física de los usuarios en caso de algún robo premeditado o intencional para la extracción de información, a fin de tratar de obtener llaves de cifrado para extraer o manipular información contenida en los equipos, lo que, según refiere, encuadra en el artículo 113, fracción V de la Ley General de Transparencia.*
- *Dar a conocer los nombres comerciales de los sistemas informáticos utilizados para el cifrado de archivos puede permitir a los 'ciber delincuentes' encontrar las llaves para su descifrado en el mercado negro.*
- *Los archivos almacenados en los equipos contienen información relacionada con las funciones desarrolladas por los servidores públicos el Alto Tribunal, en el ámbito de competencia que corresponda.*
- *En cuanto a la cantidad de puertos 'USB', la norma 'ISO 27002', que se refiere al estándar internacional para la seguridad de la información, indica diversas recomendaciones sobre prácticas en la gestión de la seguridad de la información para iniciar, implementar o mantener sistemas de gestión de la información, agrega que el uso de la información móvil implica considerar los riesgos de trabajar en entornos desprotegidos, estableciendo que se deben adoptar las medidas de seguridad adecuadas para la protección contra riesgos derivados del uso de los recursos informáticos, entre ellos, el uso de los dispositivos 'USB'.*

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

- *Conforme al Acuerdo General de Administración IV/2008, la Dirección General de Tecnologías de la Información puede restringir el acceso a un recurso como los puertos 'USB', considerando las medidas de seguridad aplicables y reservándose la difusión de esas medidas, además, porque a través de esos puertos se puede insertar algún virus, programa informático o información maliciosa que perjudique a los servidores públicos y a la institución.*

Ahora bien, como se adelantó, conforme a los argumentos reseñados se clasifica la información solicitada como ***reservada****, al estimar actualizada la hipótesis del artículo 113, fracción I de la Ley General de Transparencia, bajo el argumento central de que se podría vulnerar la seguridad y operatividad de la infraestructura tecnológica que sirve de apoyo al desarrollo de la operación de las áreas del Alto Tribunal, por lo que se transcribe ese precepto:*

> ***'Artículo 113.*** *Como información reservada podrá clasificarse aquella cuya publicación:*
> *I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;'*
> *(…)*

Al respecto, se tiene en cuenta lo resuelto en la clasificación de información CT-CI/A-3-2018, en la que este Comité determinó que los datos de cada uno de los equipos de cómputo en posesión de la Suprema Corte de Justicia de la Nación atinentes a las características de tecnología, se debían clasificar como información reservada, de conformidad con el artículo 113, fracción I de la Ley General de Transparencia, entre ellos, lo relativo al número de serie.

Se afirma que se actualiza esa hipótesis, al considerar que la Dirección General de Tecnologías de la Información es el área técnica para pronunciarse sobre la información solicitada y ha señalado que se podría comprometer la seguridad informática al proporcionar la información solicitada en relación con el número de serie de cada uno de los equipos de cómputo, pues implicaría, por ejemplo, dar a conocer que los archivos almacenados en un disco duro que tienen algún cifrado y que son controlados por contraseña, así como indicar que los usuarios no pueden copiar ni borrar archivos sin necesidad de contar con privilegios o contraseñas, lo cual, se reitera, podría poner en riesgo la seguridad y operatividad de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal, ocurriendo lo mismo si se da a conocer los nombres comerciales de los sistemas informáticos utilizados para el cifrado de archivos, pues permitiría a los 'ciber delincuentes' encontrar las llaves para su descifrado.

Para explicar esta conclusión, debe tenerse en cuenta que de conformidad con lo dispuesto en los artículos 100, último párrafo de la Ley General[3]*, en relación con el 17, párrafo primero Acuerdo General de*

[3] Corresponde al pie de página número 2 del documento original.
'Artículo 100. *…*
…
Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en esta Ley, la Ley Federal y de las Entidades Federativas."

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

Administración 5/2015[4], es competencia del titular de la instancia que tiene bajo su resguardo la información requerida, determinar su disponibilidad y clasificarla conforme a los criterios establecidos en la normativa aplicable.

Así, conforme a lo anterior, se reitera, la Dirección General de Tecnologías de la Información es la única área técnica que cuenta con el personal especializado para velar por la seguridad de la información contenida en los sistemas tecnológicos del Alto Tribunal.

En ese sentido, tratándose de cuestiones que atañen a la protección específica de los rubros que involucran aspectos vinculados con la seguridad de los sistemas tecnológicos del Alto Tribunal, es claro que cuando el área enteramente responsable de ellos ubica el surgimiento de elementos que inciden en la dimensión ya señalada, el órgano encargado de conocer del acceso sólo debe limitarse a entender y valorar la razonabilidad de la clasificación expresada para efecto de su confirmación o no.

De igual manera, como se mencionó en la resolución CT-CI/A-3-2018, en este caso, este Comité de Transparencia identifica que se pretende proteger, desde un esquema global, los equipos de cómputo a través de los cuales se desarrollan las diversas actividades de la Suprema Corte de Justicia de la Nación, pues en el caso concreto, implicaría dar conocer si los archivos almacenados en disco duro con algún cifrado son controlados por contraseña, permitiendo acceder a la información contenida en esos equipos de cómputo, lo que potencializaría el nivel de vulnerabilidad de un ataque cibernético y suplantación de identidad.

Con base en lo hasta aquí dicho, este Comité estima que la clasificación antes advertida también se sustenta, desde la especificidad que en aplicación de la prueba de daño mandatan los artículos 103 y 104 de la Ley General, cuya delimitación, como se verá enseguida, necesariamente debe responder a la propia dimensión del supuesto de reserva con el que se relacione su valoración.

Lo anterior es así, porque se podrían poner en riesgo cuestiones de seguridad pública, ya que, según se refirió previamente, dar a conocer si los archivos almacenados en un disco duro con algún cifrado son controlados por contraseña, en relación con el número de serie específico de cada equipo, así como indicar si los usuarios pueden copiar o borrar archivos sin necesidad de contar con privilegios o contraseñas, posibilitaría obtener diversa información que identificaría claramente las tecnologías, esquemas de conectividad y de seguridad, así como equipos y tecnologías que se emplean en el Alto Tribunal, facilitando acciones de posibles ataques cibernéticos.

En ese orden de ideas, se debe clasificar como reservada la información solicitada, con fundamento en la fracción I del artículo 113 de la

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

[4] Corresponde al pie de página número 3 del documento original.
'Artículo 17
De la responsabilidad de los titulares y los enlaces
En su ámbito de atribuciones, los titulares de las instancias serán responsables de la gestión de las solicitudes, así como de la veracidad y confiabilidad de la información…"

Ley General de Transparencia, por un plazo de cinco años, atendiendo a lo establecido en el artículo 101[5], de la Ley General de Transparencia.

Lo anterior no implica una limitación al derecho de acceso a la información, en tanto que el conocimiento relacionado con las tecnologías y equipos de cómputo de este Alto Tribunal, así como cualquier otro tipo de bienes o servicios tecnológicos, puede ser objeto de escrutinio público, es decir, puede obtenerse información de diversas maneras, sin la necesidad de que se proporcionen elementos que lleven a poner en riesgo la seguridad informática del Alto Tribunal, ni la información contenida en dichos equipos o sistemas como ocurre en este caso[6].

Por lo expuesto y fundado; se,

R E S U E L V E:

***ÚNICO.** En la materia de análisis, se clasifica como reservada la información solicitada, de conformidad con lo señalado en la presente determinación."*

TERCERO. **Resolución en cumplimiento del recurso de revisión.** En atención a la resolución emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en el recurso de revisión RRA 10276/18[7], el trece de marzo de dos

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

---

[5] 'Corresponde al pie de página número 4 del documento original.
Artículo 101. *Los Documentos clasificados como reservados serán públicos cuando:*
I. Se extingan las causas que dieron origen a su clasificación;
II. Expire el plazo de clasificación;
III. Exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información, o
IV. El Comité de Transparencia considere pertinente la desclasificación, de conformidad con lo señalado en el presente Título.
La información clasificada como reservada, según el artículo 113 de esta Ley, podrá permanecer con tal carácter hasta por un periodo de cinco años. El periodo de reserva correrá a partir de la fecha en que se clasifica el documento.
Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una prueba de daño.
Para los casos previstos por la fracción II, cuando se trate de información cuya publicación pueda ocasionar la destrucción o inhabilitación de la infraestructura de carácter estratégico para la provisión de bienes o servicios públicos, o bien se refiera a las circunstancias expuestas en la fracción IV del artículo 113 de esta Ley y que a juicio de un sujeto obligado sea necesario ampliar nuevamente el periodo de reserva de la información; el Comité de Transparencia respectivo deberá hacer la solicitud correspondiente al organismo garante competente, debidamente fundada y motivada, aplicando la prueba de daño y señalando el plazo de reserva, por lo menos con tres meses de anticipación al vencimiento del periodo.'
[6] Corresponde al pie de página número 5 del documento original.
Para tal efecto puede consultarse la Plataforma Nacional de Transparencia, en la siguiente liga: http://consultapublicamx.inai.org.mx:8080/vut-web/
Llenar los campos de: 'Entidad Federativa con Federación'; Sujeto Obligado con 'Suprema Corte de Justicia de la Nación'; Ley con 'Ley General de Transparencia y Acceso a la Información Pública_Ámbito Federal'; Artículo con 'Art. 70- En la Ley federal y de las Entidades federativas se contemplará que los sujetos obligados pongan a disposición del…' y 'XXXIV – Inventario de bienes muebles.'
[7] Interpuesto en contra de la resolución dictada en el expediente CT-CI/A-27-2018.

mil diecinueve, se emitió la resolución CT-CUM-R/A-2-2019[8], que se transcribe en lo conducente:

> *"**II. Análisis.** Como se advierte del antecedente I, en la solicitud que da origen a este asunto se pidió que a partir del número de serie de cada uno de los equipos de cómputo en posesión de la Suprema Corte de Justicia de la Nación, se informara lo siguiente:*
>
> *a) Si los archivos almacenados en el disco duro cuentan con algún tipo de cifrado, cuyo control se efectúe por contraseñas o credenciales administrativas.*
> *b) Nombres comerciales de los programas informáticos utilizados para el cifrado.*
> *c) Si los usuarios de los equipos pueden borrar los archivos almacenados en el disco duro, sin la necesidad de contar con privilegios o contraseñas administrativas.*
> *d) Si se encuentra instalado el navegador de Internet denominado 'Tor Browser'.*
> *e) Número de puertos 'USB' habilitados para su funcionamiento.*
> *f) Si los usuarios de los equipos pueden copiar los archivos almacenados en el disco duro, a través de los puertos "USB", sin la necesidad de contar con privilegios o contraseñas administrativas.*
>
> *En seguimiento de esa solicitud, en el expediente CT-CI/A-27-2018, se confirmó la clasificación de reserva de los datos requeridos en los incisos a), b), c), e) y f), por estimarse actualizada la hipótesis prevista en el artículo 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública; además, se tuvo por atendida la solicitud respecto de lo pedido en el inciso d).*
>
> *Ahora bien, en la resolución dictada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 10276/18, se determinó, en esencia, lo siguiente:*
>
> - *No se actualiza la causal de reserva prevista en el artículo 110, fracción I de la Ley Federal de Transparencia, esto es, por seguridad nacional, respecto del número de serie de los equipos, conocer si los discos duros se encuentran encriptados, nombre comercial de los programas de encriptado de información, conocer si se pueden borrar o no archivos con o sin contraseña, y conocer si se puede almacenar información a través de los puertos USB, de cada uno de los equipos de cómputo en posesión del Alto Tribunal.*
> - *Se actualiza la causal de reserva prevista en el artículo 110, fracción VII de la Ley Federal de la materia, consistente en la obstrucción a la prevención de delitos, respecto de los datos referidos el punto anterior.*

[8] Disponible en https://www.scjn.gob.mx/sites/default/files/resoluciones/2019-03/CT-CUM-R-A-2-2019.pdf

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

En cumplimiento de lo determinado por el Instituto Nacional de Transparencia, en el sentido de que este Comité debe dictar una resolución en la que confirme la reserva temporal de la información solicitada con fundamento en la fracción VII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, se procede a emitir el pronunciamiento correspondiente, por lo que se transcribe dicho artículo:

> *'**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:*
> *(…)*
> ***VII.** Obstruya la prevención o persecución de los delitos;'*
> *(…)*

*Sobre el alcance de dicho precepto, en la resolución emitida en el recurso de revisión que se cumplimenta, se señala que 'como información reservada podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de delitos', agregando que 'para que pueda acreditarse que la información requerida pudiera 'obstruir la prevención de los delitos', debe vincularse a la **afectación a las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos'** (página 98, vuelta).*

*Además, se precisa que de esa causal de reserva se desprenden dos vertientes: una que se refiere a la prevención de los delitos y la otra a la persecución de los mismos, agregando: 'por definición de la palabra **prevención** se hace referencia a medidas y acciones dispuestas con anticipación con el fin de evitar o impedir que se presente un fenómeno peligroso para reducir sus efectos sobre la publicación', de ahí que 'prevención del delito' significa 'tomar medidas y realizar acciones para evitar una conducta o un comportamiento que puedan dañar o convertir a la población en sujetos o víctimas de un ilícito' y que desde el punto de vista criminológico prevenir es 'conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla; es decir, no permitir que alguna situación llegue a darse porque ésta se estima inconveniente'.*

*Enseguida se hace alusión al Código Penal Federal señalando que 'comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, sean o no propiedad del Estado. Asimismo, al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del **Estado**, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa' (foja 100 vuelta).*

Adicionalmente, es de destacar que en la resolución emitida por el Instituto Nacional de Transparencia que se atiende, se invoca como hecho notorio, las respuestas que la Dirección General de Tecnologías de la Información de ese Instituto emitió en respuesta a las consultas que se le

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

formularon sobre información similar a la de la materia de la solicitud que da origen a este asunto.[9]

En virtud de lo anterior, en la resolución se argumenta que 'derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, y que se trata de un elemento relevante al ponderar cualquier posible vulneración a la seguridad de la infraestructura tecnológica de la autoridad obligada, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática ***perturben el sistema de la infraestructura tecnológica*** *de la Suprema Corte de Justicia de la Nación, ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un estado vulnerable la información que en ella se contiene, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información; resultando, por lo tanto, es procedente su reserva', conforme al artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en específico, la obstrucción a la prevención de delitos.*

De conformidad con lo expuesto, atendiendo a los argumentos señalados por el Instituto Nacional de Transparencia, este Comité de Transparencia ***confirma la clasificación de reserva*** *de la información relativa al número de serie; conocer si los discos duros se encuentran encriptados; nombre comercial de los programas de encriptado de información; conocer si pueden borrar o no archivos con o sin contraseñas, y conocer si se puede almacenar información a través de los puertos USB, de cada uno de los equipos de cómputo en posesión de la Suprema Corte de Justicia de la Nación,*

---

[9] Corresponde al pie de página número 1 del documento original.
'Sin embargo, añadió que ***cuando se proporciona un conjunto de datos informáticos de TIC sensibles y que además se encuentran correlacionados, como los peticionados****, con tal información cualquier persona con* ***fines malintencionados****, podría utilizar sus conocimientos para 'hackear' (acción de entrar de forma abrupta y sin permiso a un sistema de cómputo o una red) o crackear (literalmente traducido como rompedor, del inglés ' to track', que significa romper o quebrar) se utiliza para referirse a las personas que rompen o vulneran algún sistema de seguridad, los sistemas informáticos objetivo y de alguna manera correlacionan la información para* ***vulnerar la seguridad de los equipos informáticos así como afectar los servicios informáticos del sujeto obligado'*** *(foja 101 vuelta).*'
En el desahogo de diversa consulta, la citada unidad administrativa expuso:

- ✓ *'Que en criptografía, el cifrado es un procedimiento que utiliza un algoritmo con 'clave descifrado' para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave de cifrado del algoritmo. Las claves de cifrado y descifrado pueden ser simétricas, asimétricas o híbridas.*
- ✓ *Que dentro de las Tecnologías de la Información y Comunicación, el* ***cifrado de disco duro proporciona una capa de seguridad con la finalidad de proteger información sensible*** *y que únicamente aquellas personas que posean la clave de cifrado puedan leer y editar información. Por tanto, el cifrado de disco duro protege la información contenida dentro del mismo, en el caso de que una persona ajena tenga acceso físico a nuestro equipo.*
- ✓ *Por otro lado, si se extrae el disco duro y este es montado en otro equipo de cómputo, la información contenida dentro de su interior no podrá ser leída.'*

De igual forma, respecto del cuestionamiento '¿Dar a conocer si los archivos almacenados están cifrados, y los nombres comerciales de los programas informáticos para el cifrado utilizados por el sujeto obligado, representan un riesgo a los sistemas, redes o equipos del sujeto obligado?', la dirección general en comento refirió (foja 102):

> *'Cuando se proporciona un conjunto de datos informáticos de TIC sensibles y que además se encuentran correlacionados como por ejemplo:* ***nombres comerciales de los programas informáticos para cifrar****, método de cifrado, tipo de cifrado, longitud de las llaves, etc., con tal información* ***cualquier persona con fines malintencionados, podría utilizar sus cocimientos o contratar alguna persona con capacidades y conocimientos en materia de hackear'***
> *(…)'*

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

con fundamento en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, dado que como se hizo valer en la resolución dictada en el expediente CT-CI/A-27-2018, considerando que la Dirección General de Tecnologías de la Información es el área técnica para pronunciarse sobre la información solicitada y señaló que se podría comprometer la seguridad informática al proporcionar la información solicitada en relación con el número de serie de cada uno de los equipos de cómputo, implicaría, por ejemplo, dar a conocer que los archivos almacenados en un disco duro que tienen algún cifrado y que son controlados por contraseña, así como indicar que los usuarios no pueden copiar ni borrar archivos sin necesidad de contar privilegios o contraseñas, podría poner en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal, ocurriendo lo mismo si se da a conocer los nombres comerciales de los sistemas informáticos utilizados para el cifrado de los archivos.

Dado que, conforme a la argumentación sostenida en la resolución del Instituto Nacional de Transparencia que se atiende la reserva de dicha información permite prevenir la comisión del delito de acceso ilícito a sistemas y equipos de informática tipificados en el Código Penal Federal, pues al dar a conocer la información solicitada, no sólo se 'comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional'.

Por lo tanto, se confirma se confirma la reserva de la información requerida, en los incisos a), b), c), e) y f) de la solicitud, con fundamento en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

***Análisis específico de la prueba de daño**. En el caso, de acuerdo con el alcance de la causa de reserva prevista en el artículo 110, fracción VI de la Ley Federal de Transparencia y en términos de lo señalado por el Instituto Nacional de Transparencia en el recurso de revisión que se atiende, se determina (fojas 102 vuelta y 103):*

La divulgación de la información solicitada conllevaría un riesgo real, demostrable e identificable, en tanto que colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad, facilitando una posible intervención de las comunicaciones; usurpación de permisos; suplantación de equipos y de la información almacenada en los servidores; robo de información que obran en los archivos digitales, así como el detrimento de las instalaciones tecnológicas.

*En ese sentido, el perjuicio significativo al **interés público** resulta **menos restrictivo**, porque se pondría en riesgo la responsabilidad fundamental del Alto Tribunal en la defensa del orden establecido en la Constitución Federal, mediante los medios de control constitucional.*

*Por lo anterior, acorde con la resolución que se atiende se determinó que '**el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información**, ya que el resguardo de los datos consistentes en los **números de serie** de los equipos de cómputo y*

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

*los **nombres comerciales de los programas informáticos utilizados para el cifrado de los archivos** instalados en los equipos de la dependencia, implica llevar a cabo la **prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal**, lo cual cobra importancia si se considera que dicha conducta implica conocer, copias, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática', por lo que revelar dichos datos 'no sólo se comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional'.*

*Ahora bien, dicha clasificación de reserva '**se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio,** toda vez que **la pretensión de fondo que persigue la reserva de la información consiste en prevenir la conducta antijurídica tipificada** (acceso ilícito a sistemas y equipos de informática)', de llevarse a cabo podría permitir la ejecución de diversos **ataques** a la infraestructura tecnológica y de sistemas con que cuenta este Alto Tribunal, ya que la difusión de los documentos solicitados '**incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito'**, pues tendría acceso a información con un alto grado de precisión técnica, así como a los protocolos de seguridad y las características de la infraestructura instalada (foja 103).*

***Plazo de reserva.** Finalmente, en términos de lo señalado en el artículo 101, párrafo segundo de la Ley General de Transparencia, se determina que el plazo de reserva será por cinco años, ya que por las consideraciones expuestas en la resolución del Instituto Nacional de Transparencia, mismas que se retoman en esta determinación, 'dicho plazo es proporcional a la naturaleza y el grado de especificidad del tipo de información de que se trata'.*

En cumplimiento de la determinación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales hágase del conocimiento del solicitante esta determinación, la cual también deberá hacerse llegar a ese órgano garante, ya que contiene los motivos que sustentan la clasificación de reserva en los términos expuestos en el recurso de revisión que se atiende respecto de la información requerida.

Por lo expuesto y fundado; se,

R E S U E L V E:

***PRIMERO.** Se confirma la clasificación de reserva temporal de la información materia del recurso de revisión que se cumplimenta, acorde con lo señalado en esta resolución.*

***SEGUNDO.** De conformidad con lo expuesto en la presente resolución, se atiende lo determinado por el Instituto Nacional de Transparencia.*

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

> ***TERCERO.*** *Se instruye a la Unidad General de Transparencia informar lo conducente al Instituto Nacional de Transparencia y al solicitante, así como realizar las acciones necesarias para atender este asunto.”*

CUARTO. Requerimiento para actualizar el índice de información reservada. Mediante oficio CT-578-2023, enviado por correo electrónico el veintiuno de septiembre de dos mil veintitrés, la Secretaría Técnica de este Comité de Transparencia solicitó a la Dirección General de Tecnologías de la Información (DGTI) que se pronunciara sobre la vigencia de la reserva de la información clasificada en la resolución de cumplimiento antes transcrita, o bien, si procedía su desclasificación.

QUINTO. Informe de la DGTI, sobre el seguimiento al índice de información reservada. El cinco de octubre de dos mil veintitrés, se remitió por el Sistema de Gestión Documental, el oficio DGTI/466/2023, con el que el titular de la DGTI remite la Atenta Nota de Cumplimiento números DGTI/SGST-0018-2023 y DGTI/DSI-19-2023, del Subdirector General de Servicios Tecnológicos, del Director de Seguridad Informática y del Subdirector de Ciberseguridad, en la que se informa:

> (…)
> *“Al respecto, se informa que subsisten las causas que dieron origen a la clasificación de la información, con fundamento en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y la fracción VII del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, como a continuación se expone:*
>
> *Conforme al artículo 111 de la Ley Federal de Transparencia y Acceso a la Información Pública los sujetos obligados deben fundar y motivar las causales de reserva previstas en el artículo 110 de dicho ordenamiento, a través de la aplicación de la prueba de daño a la que se refiere el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública. Por su parte, el mencionado artículo 104 establece que, en la justificación de la prueba de daño, el sujeto obligado deberá corroborar lo siguiente:*
>
> *a) Que la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.*

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

b) Que el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda.

c) Que la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

Por otra parte, el Trigésimo Tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos Generales), establece que:

> *'Para la aplicación de la prueba de daño a la que hace referencia el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, los sujetos obligados atenderán lo siguiente:*
>
> *I. Se debe citar la fracción y, en su caso, la causal aplicable del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, vinculándola con el Lineamiento específico y, cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada.*
> *II. Mediante la ponderación de los intereses en conflicto, los sujetos obligados deben demostrar que la publicidad de la información solicitada generaría un riesgo de perjuicio y por lo tanto, tendrán que acreditar que este último rebasa el interés público protegido por la reserva.*
> *III. Se debe de acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate.*
> *IV. Precisar las razones objetivas por las que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable.*
> *V. En la motivación de la clasificación, el sujeto obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño.*
> *VI. Deberán elegir la opción de excepción al acceso a la información que menos lo restrinja, la cual será adecuada y proporcional para la protección del interés público, y deberá interferir lo menos posible en el ejercicio efectivo del derecho de acceso a la información.'*

Bajo este contexto, debe señalarse que, la normativa instituye las causales de reserva y establece como mecanismo para fundar y motivar tales causales, la aplicación de una prueba de daño que deben proporcionar los sujetos obligados para acreditarse el cumplimiento de elementos que se señalan en el Trigésimo Tercero de los Lineamientos Generales.

Por su parte, el artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública prevé la posibilidad para los sujetos obligados de ampliar el plazo de reserva siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una prueba de daño.

Por lo anterior, y a fin de fundar y motivar la ampliación del periodo de reserva de la información, se informa que subsisten las causas que dieron origen a la clasificación de la información, por lo que se aplica la siguiente prueba de daño:

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

- *Existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público, ya que, colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad, facilitando una posible intervención de las comunicaciones; usurpación de permisos; suplantación de equipos y de la información almacenada en los servidores; robo de información que obran en los archivos digitales, así como al detrimento de las instalaciones tecnológicas. Dichas cuestiones podrían materializarse con la comisión de delitos de carácter cibernético, que sin duda afectarían severamente el ejercicio de las labores cotidianas y sustantivas de la Suprema Corte de Justicia de la Nación.*

- *Se supera el interés público general de que se difunda la información, ya que el resguardo de los datos consistentes en los números de serie de los equipos de cómputo y los nombres comerciales de los programas informáticos utilizados para el cifrado de los archivos instalados en los equipos de esta Suprema Corte, implica llevar a cabo la prevención del delito de acceso ilícito a sistemas y equipos de informática, tipificado en el Código Penal Federal, lo cual cobra importancia si se considera que dicha conducta implica 'conocer, copias* (sic)*, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática', por lo que, revelar dichos datos no sólo se comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional.*

- *El proteger la información clasificada como reservada se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que, la pretensión de fondo que persigue, el que la información continue siendo reservada, consiste en prevenir la conducta antijurídica tipificada (acceso ilícito a sistemas y equipos de informática), de llevarse a cabo podría permitir la ejecución de diversos ataques a la infraestructura tecnológica y de sistemas con que cuenta este Alto Tribunal, ya que la difusión de los documentos solicitados 'incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito', pues tendría acceso a información con un alto grado de precisión técnica, así como a los protocolos de seguridad y las características de la infraestructura instalada.*

Derivado de todo lo anterior, cabe precisar que el Código Penal Federal[10] *dispone lo siguiente:*

'Acceso ilícito y equipos de informática

[10] *Disponible para consulta en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf*

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

> *ARTICULO 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún* mecanismo *de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.*
>
> *ARTICULO* 211 *BIS 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días de multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.*
>
> *A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.*
> *…*
>
> *ARTICULO 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.'*

De los preceptos referidos, se advierte que comete el delito de acceso ilícito a sistemas y equipo de informática, todo aquel que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean o no propiedad del Estado.

Asimismo, mencionan que, a quien sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.

En conclusión, es procedente ampliar la reserva de la información, ya que subsisten las causas que dieron origen a su clasificación, con fundamento en los artículos 99, tercer párrafo y 110, fracción VII de la Ley Federal de

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

Transparencia y Acceso a la Información Pública y la fracción VII del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública.

Ahora bien, en cuanto al periodo de reserva, el mencionado artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Trigésimo Cuarto de los Lineamientos Generales, establecen que la información clasificada podrá permanecer con tal carácter, hasta por un periodo de cinco años, y que tal información podrá ser desclasificada:

a) cuando se extingan las causas que dieron origen a su clasificación;
b) cuando expire el plazo de clasificación;
c) cuando exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información;
d) cuando el Comité de Transparencia considere pertinente la desclasificación de conformidad con el Título cuarto del mismo ordenamiento, o
e) cuando se trate de información que esté relacionada con violaciones graves a derechos humanos o delitos de lesa humanidad.

Por otra parte, el tercer párrafo del artículo 99 antes mencionado señala:

> *'Artículo 99. (…)*
>
> *Fracciones I a V (…)*
>
> *(…)*
>
> *Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una prueba de daño.*
>
> *(…)'*

En el caso concreto, considerando la aplicación de la prueba de daño, se justifica que prevalecen las causas que originaron la reserva y por ello el periodo debe ampliarse hasta por un plazo de cinco años adicionales.

Por último, todo lo anteriormente expuesto, se refuerza con lo resuelto por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en sesión del veinte de febrero de dos mil diecinueve, en el recurso de revisión RRA 10276/18, en el cual resalta lo siguiente:

> *'(…) se determina que en el presente caso no se actualiza la causal de reserva prevista en el artículo 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública.*

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

No obstante, tomando en cuenta la naturaleza de la información y de los argumentos esgrimidos por el sujeto obligado en vía de alegatos, con fundamento en el artículo 147 de la Ley General de Transparencia y Acceso a la Información Pública, se procede a analizar la causal de reserva establecida en la fracción VII, del artículo 110, de la Ley Federal de Transparencia y Acceso a la Información Pública, misma que prevé:

'Artículo 110. Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada *podrá clasificarse aquella cuya publicación:*
…
VII. Obstruya la prevención o persecución de los delitos;'

Así, este Instituto considera que la entrega de dichos datos se ocasionaría lo siguiente:

I. Un potencial ***riesgo real, demostrable e identificable*** *a la Suprema Corte de Justicia de la Nación, toda vez que, se le colocaría en un estado de* ***vulnerabilidad*** *que permitiría el acceso a sus sistemas y equipos informáticos facilitando:*

a. *Una posible intervención de sus comunicaciones,*
b. *La usurpación de sus permisos,*
c. *La suplantación de sus equipos y de la información que almacena en sus servidores;*
d. *El robo de la información que obra en sus archivos digitales, y*
e. *El detrimento de sus instalaciones tecnológicas.*

Cuestiones que se materializan con la comisión de delitos de carácter cibernético, que sin duda afectarían severamente el ejercicio de las labores cotidianas y sustantivas de la Suprema Corte de Justicia de la Nación.

II. Un ***perjuicio significativo al interés público****, ya que se pondría en riesgo su responsabilidad fundamental en la defensa del orden establecido por la Constitución Política de los Estados Unidos Mexicanos, a través de los medios de control constitucional.*

Con base en lo anterior, ***el riesgo de perjuicio que supondría la divulgación supera el interés público general*** ***de que se difunda la información****, ya que el resguardo de los datos consistentes en los* ***números de serie*** *de los equipos de cómputo y los* ***nombres comerciales de los programas informáticos utilizados para el cifrado*** ***de los archivos*** *instalados en los equipos de la dependencia, implica llevar a cabo la* ***prevención del delito de*** ***acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal****, lo cual cobra importancia si se considera que dicha conducta implica conocer, copias, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática. (sic)*

En consecuencia, al revelar dichos datos no sólo se comprometería la información que obra en los archivos digitales del sujeto obligado, sino que

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional.

*Asimismo, **la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio**, toda vez que **la pretensión de fondo que persigue la reserva de la información consiste en prevenir la conducta antijurídica tipificada** (acceso ilícito a sistemas y equipos de informática), misma que de llevarse a cabo podría permitir la realización de diversos **ataques** a la infraestructura tecnológica y de sistemas del sujeto obligado.*

Por todo lo anterior, se advierte que difundir información relativa a los números de serie de los equipos y la versión del firewall instalado, incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado, conociendo con un alto grado de precisión la información técnica referente a sus equipos de cómputo, los protocolos de seguridad y las características de la infraestructura instalada.

*…este Organismo Garante del derecho de acceso a la información pública **concluye que procede la reserva** de la información relativa al número de serie, el conocer si los discos duros se encuentran encriptados, el nombre comercial de los programas de encriptado de información, conocer si pueden borrar o no archivos con o sin contraseñas y conocer si se puede almacenar la información a través de los puertos USB, de cada uno de los equipos de cómputo en posesión del sujeto obligado, **de conformidad con lo previsto en el artículo 110, fracción VII** de la Ley Federal de Transparencia y Acceso a la Información Pública.* (sic)

Por otra parte, el propio Comité de Transparencia de la Suprema Corte de Justicia de la Nación, a través de la resolución del expediente de cumplimiento CT-CUM-R/A-2-2019, derivado del CT-CI/A-27-2018, señala lo siguiente:

‘…De conformidad con lo expuesto, atendiendo a los argumentos señalados por el Instituto Nacional de Transparencia, este Comité de Transparencia confirma la clasificación de reserva de la información relativa al número de serie; conocer si los discos duros se encuentran encriptados; nombre comercial de los programas de encriptado de información; conocer si pueden borrar o no archivos con o sin contraseñas, y conocer si se puede almacenar información a través de los puertos USB, de cada uno de los equipos de cómputo en posesión de la Suprema Corte de Justicia de la Nación, con fundamento en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, dado que como se hizo valer en la resolución dictada en el expediente CT-CI/A-27-2018, considerando que la Dirección General de Tecnologías de la Información es el área técnica para pronunciarse sobre la información solicitada y señaló que se podría comprometer la seguridad informática al proporcionar la información solicitada en relación con el número de serie de cada uno de los equipos de cómputo, implicaría, por ejemplo, dar a conocer que los archivos almacenados en un disco duro que tienen algún

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

cifrado y que son controlados por contraseña, así como indicar que los usuarios no pueden copiar ni borrar archivos sin necesidad de contar privilegios o contraseñas, podría poner en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal, ocurriendo lo mismo si se da a conocer los nombres comerciales de los sistemas informáticos utilizados para el cifrado de los archivos.

Dado que, conforme a la argumentación sostenida en la resolución del Instituto Nacional de Transparencia que se atiende la reserva de dicha información permite prevenir la comisión del delito de acceso ilícito a sistemas y equipos de informática tipificados en el Código Penal Federal, pues al dar a conocer la información solicitada, no sólo se comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional.

Por lo tanto, se confirma se confirma (sic) *la reserva de la información requerida, en los incisos a), b), c), e) y f) de la solicitud, con fundamento en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. (sic)*

***Análisis específico de la prueba de daño**. En el caso, de acuerdo con el alcance de la causa de reserva prevista en el artículo 110, fracción VI de la Ley Federal de Transparencia y en términos de lo señalado por el Instituto Nacional de Transparencia en el recurso de revisión que se atiende, se determina (fojas 102 vuelta y 103):*

La divulgación *de la **información solicitada conllevaría un riesgo real, demostrable e identificable,** en tanto que colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad, facilitando una posible intervención de las comunicaciones; usurpación de permisos; suplantación de equipos y de la información almacenada en los servidores; robo de información que obran* (sic) *en los archivos digitales, así como el detrimento de las instalaciones tecnológicas.*

*En ese sentido, el perjuicio significativo **al interés público** resulta **menos restrictivo**, porque se pondría en riesgo la responsabilidad fundamental del Alto Tribunal en la defensa del orden establecido en la Constitución Federal, mediante los medios de control constitucional.*

Por lo anterior*, acorde con la resolución que se atiende se determinó que '**el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información**, ya que el resguardo de los datos consistentes en los **números de serie** de los equipos de cómputo y los **nombres comerciales de los programas informáticos utilizados para el cifrado de los archivos** instalados en los equipos de la dependencia, implica llevar a cabo la **prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal**, lo cual cobra importancia si se considera que dicha conducta implica conocer, copias* (sic)*, modificar, destruir o provocar la pérdida de información contenida en sistemas*

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

> *o equipos de informática', por lo que revelar dichos datos no sólo se comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional.*
>
> *Ahora bien, dicha clasificación de reserva '**se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir la conducta antijurídica tipificada** (acceso ilícito a sistemas y equipos de informática)', de llevarse a cabo podría permitir la ejecución de diversos ataques a la infraestructura tecnológica y de sistemas con que cuenta este Alto Tribunal, ya que la difusión de los documentos solicitados '**incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito**', pues tendría acceso a información con un alto grado de precisión técnica, así como a los protocolos de seguridad y las características de la infraestructura instalada (…)' (foja 103)."*

SEXTO. Acuerdo de turno. Mediante proveído de cinco de octubre de dos mil veintitrés, la Presidencia del Comité de Transparencia de este Alto Tribunal, con fundamento en los artículos 44, fracción VIII, 101, 103 y 27, del Acuerdo General de Administración 5/2015, ordenó integrar el expediente de cumplimiento **CT-CUM/A-47-2023** y remitirlo al Contralor del Alto Tribunal, lo que se hizo mediante oficio CT-617-2023, enviado por correo electrónico de seis de octubre de este año.

C O N S I D E R A C I O N E S:

PRIMERA. Competencia. El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para pronunciarse sobre la ampliación del periodo de reserva de la información, en términos de los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos, 4 y 44, fracción VIII, y 101, párrafo tercero, de la Ley General de Transparencia y Acceso a Información Púbica (Ley General de Transparencia), así como 23, fracción I, del Acuerdo General de Administración 5/2015.

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

SEGUNDA. Análisis. En la solicitud que da origen a este asunto se pidió que, a partir del número de serie de cada uno de los equipos de cómputo en posesión de la SCJN, se informara:

a) Si los archivos almacenados en el disco duro cuentan con algún tipo de cifrado, cuyo control se efectúe por contraseñas o credenciales administrativas.
b) Nombres comerciales de los programas informáticos utilizados para el cifrado.
c) Si los usuarios de los equipos pueden borrar los archivos almacenados en el disco duro, sin la necesidad de contar con privilegios o contraseñas administrativas.
d) Si se encuentra instalado el navegador de Internet denominado *"Tor Browser".*[11]
e) Número de puertos "USB" habilitados para su funcionamiento.
f) Si los usuarios de los equipos pueden copiar los archivos almacenados en el disco duro, a través de los puertos "USB", sin la necesidad de contar con privilegios o contraseñas administrativas.

En cumplimiento de la resolución dictada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 10276/18, en el expediente CT-CUM-R/A-2-2019 se confirmó la reserva de la información concerniente a los incisos a), b), c), e) y f), de conformidad con los artículos 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal de Transparencia) y 113, fracción VII, de la Ley General de

[11] Este aspecto no fue materia de la resolución CT-CUM-R/A-2-2019, porque se tuvo por atendido en la resolución CT-CI/A-27-2018.

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

Transparencia, pues la publicidad de esa información puede obstruir la prevención de delitos, conforme a los argumentos que se reseñan:

- Es reservada aquella información cuya publicación obstruya la prevención o persecución de delitos, por lo que para acreditar que la información obstruye la prevención de los delitos, debe vincularse con la afectación a las acciones implementadas por las autoridades para evitar su comisión o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.
- Conforme al Código Penal Federal se *"comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, sean o no propiedad del Estado. Asimismo, al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del **Estado**, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa"*.
- Derivado de la naturaleza y el grado de especificidad de la información que nos ocupa y de que se trata de un elemento relevante al ponderar cualquier posible vulneración a la seguridad de la infraestructura tecnológica de la SCJN, se concluye que darla a conocer facilitaría que personas expertas en informática perturben la infraestructura tecnológica de la SCJN, ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante, lo que pondría en un estado vulnerable la información que contienen, facilitando la

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información.

- La DGTI es el área técnica de la SCJN con atribuciones para pronunciarse sobre dicha información y señaló que se podría comprometer la seguridad informática, pues proporcionar el número de serie de cada uno de los equipos de cómputo, implicaría, por ejemplo, dar a conocer que los archivos almacenados en un disco duro que tienen algún cifrado y que son controlados por contraseña, así como indicar que los usuarios no pueden copiar ni borrar archivos sin necesidad de contar privilegios o contraseñas, podría poner en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal, ocurriendo lo mismo si se da a conocer el nombre comercial de los sistemas informáticos utilizados para el cifrado de los archivos.
- Con base en los argumentos expuestos, se consideró procedente la reserva de la información, con apoyo en el artículo 110, fracción VII, de la Ley Federal de Transparencia, por un plazo de cinco años.

Considerando que el plazo de reserva de la información estaba próximo a vencer, la Secretaría de este Comité de Transparencia solicitó a la DGTI que se pronunciara sobre si prevalecía la reserva o si procedía su desclasificación y, en respuesta a ello, señaló que subsisten las causas que dieron origen a la clasificación de la información y que el plazo es susceptible de ampliarse por cinco años.

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

Al respecto, la DGTI añade en el informe que, sobre la prueba de daño prevista en el artículo 104[12] de la Ley General de Transparencia, los siguientes aspectos a considerar:

- La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público, pues colocaría a la SCJN en un estado de vulnerabilidad facilitando una posible intervención de las comunicaciones, usurpación de permisos, suplantación de equipos y de la información almacenada en los servidores; robo de información que obra en los archivos digitales, así como el detrimento de las instalaciones tecnológicas, lo que constituye un riesgo real de que se cometan delitos cibernéticos, afectando, severamente, el ejercicio de las labores cotidianas y sustantivas de la SCJN.
- El riesgo de perjuicio que supondría la divulgación de la información supera el interés público general de que se difunda, porque el resguardo de los datos consistentes en el número de serie de los equipos de cómputo y el nombre comercial de los programas informáticos utilizados para el cifrado de los archivos instalados en los equipos de la SCJN, implica llevar a cabo la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal, lo que cobra importancia si se considera que dicha conducta implica *“conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática”*, por lo que revelar esos datos no solo comprometería la información que obra en los archivos digitales, sino que implica

[12] *“**Artículo 104.** En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*
I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;
II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y
III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.”

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

un menoscabo a la seguridad y certeza de las personas que acuden a la SCJN respecto de la impartición de justicia y control constitucional.

- La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, porque lo que se pretende es que la información continue siendo reservada, para prevenir una conducta antijurídica tipificada, "*acceso ilícito a sistemas y equipos de informática*", la cual, de llevarse a cabo, podría permitir la ejecución de diversos ataques a la infraestructura tecnológica y de sistemas con que cuenta la SCJN.
- En otras palabras, la difusión de la información materia de la solicitud de origen "*incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito"*, pues se otorgaría acceso a información con un alto grado de precisión técnica, así como a los protocolos de seguridad y las características de la infraestructura instalada, por lo que procede la ampliación del plazo de reserva de la información solicitada, con apoyo en los artículos 99, tercer párrafo y 110, fracción VII, de la Ley Federal de Transparencia y 113, fracción VII, de la Ley General de Transparencia.

Ahora bien, para emitir pronunciamiento sobre si procede ampliar el plazo de reserva de la información que nos ocupa, se tiene en cuenta que conforme a los artículos 100[13] de la Ley General de Transparencia y

[13] *"**Artículo 100.** La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.*
Los supuestos de reserva o confidencialidad previstos en las leyes deberán ser acordes con las bases, principios y disposiciones establecidos en esta Ley y, en ningún caso, podrán contravenirla.
Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en esta Ley, la Ley Federal y de las Entidades Federativas."

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

97[14] de la Ley Federal de Transparencia, en relación con el diverso 17[15] del Acuerdo General de Administración 5/2015, es competencia de los titulares de las instancias que tienen bajo resguardo la información solicitada determinar su disponibilidad, clasificarla conforme a la normativa aplicable y, en su caso, señalar el plazo de reserva.

En términos del artículo 36, fracciones I, V, VI y IX[16], del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación, la DGTI es el área técnica que cuenta con el personal especializado para velar por la seguridad de los sistemas tecnológicos de la SCJN, pues le corresponde administrar los sistemas informáticos jurídicos, administrativos y jurisdiccionales de este Alto Tribunal.

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

---

[14] "***Artículo 97.*** *La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.*
En el proceso de clasificación de la información, los sujetos obligados observarán, además de lo establecido en el Título Sexto de la Ley General, las disposiciones de la presente Ley.
Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en la Ley General y la presente Ley.
Los sujetos obligados deberán aplicar, de manera restrictiva y limitada, las excepciones al derecho de acceso a la información previstas en el presente Título y deberán acreditar su procedencia, sin ampliar las excepciones o supuestos de reserva o confidencialidad previstos en las leyes, de conformidad con lo establecido en la Ley General.
Los sujetos obligados no podrán emitir acuerdos de carácter general ni particular que clasifiquen documentos o expedientes como reservados, ni clasificar documentos antes de dar respuesta a una solicitud de acceso a la información.
La clasificación de información reservada se realizará conforme a un análisis caso por caso, mediante la aplicación de la prueba de daño."

[15] ***"Artículo 17***
De la responsabilidad de los titulares y los enlaces
En su ámbito de atribuciones, los titulares de las instancias serán responsables de la gestión de las solicitudes, así como de la veracidad y confiabilidad de la información.
A efecto de instituir un vínculo de comunicación para las gestiones derivadas de trámites de acceso a la información, protección de información reservada y/o confidencial y transparencia, los titulares de las instancias designarán un servidor público que fungirá como Enlace e informarán por escrito sobre su designación a la Unidad General."

[16] *"**Artículo 36.** La Dirección General de Tecnologías de la Información tendrá las atribuciones siguientes:*
I. Administrar los recursos en materia de tecnologías de la información y comunicación, así como proveer los servicios que se requieran en la materia;
II. Recabar las necesidades de bienes y servicios en materia de tecnologías de la información y comunicación (…)
V. Planificar, diseñar, desarrollar y mantener en operación los sistemas informáticos jurídicos, administrativos y jurisdiccionales, así como los portales y micrositios que requieran los órganos y áreas, de conformidad con las disposiciones jurídicas aplicables;
VI. Elaborar estudios técnicos en materia de infraestructura tecnológica, así como de sistemas y bienes informáticos;
(…)
IX. Instrumentar los mecanismos en materia de seguridad informática y vigilar su adecuado funcionamiento;
(…)

En ese sentido, la DGTI ha expuesto las razones por las que conforme los artículos 110, fracción VII, de la Ley Federal de Transparencia y 113, fracción VII, de la Ley General de Transparencia, considera que subsiste el riesgo real, demostrable e identificable que originó que se reservará la información señalada en los incisos a), b), c), e) y f), de la solicitud de origen, pues refiere que con la difusión del número de serie, el conocer si los discos duros se encuentran encriptados, el nombre comercial de los programas de encriptado de información, si se pueden borrar o no archivos con o sin contraseñas y si se puede almacenar información a través de los puertos USB, de cada uno de los equipos de cómputo en posesión de este Alto Tribunal, se podría generar un potencial riesgo para la infraestructura tecnológica de la SCJN, ya que podría ser utilizada para propiciar ataques informáticos.

Así, en concordancia con los argumentos expuestos en la resolución CT-CUM-R/A-2-2019, se estima que, en efecto, subsiste el riesgo real, demostrable e identificable que motivó la reserva de dicha información, con apoyo en los artículos 110, fracción VII, de la Ley Federal de Transparencia y 113, fracción VII, de la Ley General de Transparencia, puesto que la difusión de esos datos, por sí misma, representa razonablemente el riesgo de que se facilite la comisión de delitos, como puede ser el acceso ilícito a sistemas informáticos y equipos de informática.

En efecto, como se señaló en la resolución CT-CUM-R/A-2-2019, la información relativa al número de serie, vinculado con los datos referidos en los incisos a), b), c), e) y f) de la solicitud, constituye información susceptible de ser reservada, ya que darla a conocer facilitaría que personas expertas en informática intenten acceder a la infraestructura tecnológica de la SCJN, ejecuten programas informáticos perjudiciales

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

que modifiquen o destruyan información relevante y, con ello, poner en riesgo la información que en ella se contiene, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información.

Además, persiste lo señalado en el cumplimiento CT-CUM-R/A-2-2019, en el sentido de que el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información solicitada, pues el resguardo de los datos consistentes en el número de serie de los equipos de cómputo y el nombre comercial de los programas informáticos utilizados para el cifrado de los archivos instalados en los equipos de la SCJN, conlleva prevenir el delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal, lo que cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos informáticos.

Aunado a lo expuesto, con la difusión de la información requerida no solo se comprometería la información que obra en los archivos informáticos de este Alto Tribunal, sino que conlleva un menoscabo en la seguridad y certeza de las personas que acuden a la SCJN para otorgar certeza sobre la impartición de justicia y control constitucional.

Por tanto, de conformidad con los artículos 44, fracción VIII y 103, de la Ley General de Transparencia, se determina justificado ampliar el periodo de reserva sobre la información relativa al número de serie vinculado con los datos referidos en los inciso a), b), c), e) y f) de la solicitud de origen, consistentes en si los discos duros se encuentran encriptados, nombre comercial de los programas de encriptado de información, si se pueden borrar o no archivos con o sin contraseñas y si

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

se puede almacenar información a través de los puertos USB y el número de éstos, pues conforme a las razones expuestas, la divulgación de esa información obstaculizaría la prevención de delitos, lo que sigue actualizando la hipótesis de reserva prevista en los artículos 110, fracción VII, de la Ley Federal de Transparencia y 113, fracción VII, de la Ley General de Transparencia.

Prueba de daño. Conforme a lo expuesto en la resolución CT-CUM-R/A-2-2019, la divulgación de la información solicitada conllevaría un riesgo real, demostrable e identificable, en tanto que colocaría a la SCJN en un estado de vulnerabilidad, facilitando una posible intervención de las comunicaciones, usurpación de permisos, suplantación de equipos y de la información almacenada en los servidores, robo de información que obran en los archivos digitales, así como el detrimento de las instalaciones tecnológicas, por lo que el perjuicio significativo al interés público resulta menos restrictivo, porque se pondría en riesgo la responsabilidad fundamental de la SCJN en la defensa del orden establecido en la Constitución Federal, mediante los medios de control constitucional.

Respecto de la ampliación del plazo de reserva, se tiene en cuenta que el artículo 101[17] de la Ley General de Transparencia contempla la

[17] *"**Artículo 101.** Los Documentos clasificados como reservados serán públicos cuando:*
I. Se extingan las causas que dieron origen a su clasificación;
II. Expire el plazo de clasificación;
III. Exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información, o
IV. El Comité de Transparencia considere pertinente la desclasificación, de conformidad con lo señalado en el presente Título.
La información clasificada como reservada, según el artículo 113 de esta Ley, podrá permanecer con tal carácter hasta por un periodo de cinco años. El periodo de reserva correrá a partir de la fecha en que se clasifica el documento.
Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una prueba de daño.
Para los casos previstos por la fracción II, cuando se trate de información cuya publicación pueda ocasionar la destrucción o inhabilitación de la infraestructura de carácter estratégico para la provisión de bienes o servicios públicos, o bien se refiera a las circunstancias expuestas en la fracción IV del artículo 113 de esta Ley y que a juicio de un sujeto obligado sea necesario ampliar nuevamente el periodo de reserva de la información; el Comité de Transparencia respectivo deberá hacer la solicitud correspondiente al organismo garante competente, debidamente

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

posibilidad de que pueda ampliarse hasta por cinco años adicionales, cuando se justifique que prevalecen las causas que dieron origen a su clasificación, lo que en este caso ocurre; por tanto, la ampliación que se autoriza es por cinco años contados a partir del vencimiento del primer periodo de reserva, en el entendido de que ese plazo podrá concluir, previamente, siempre que se extingan las causas que dieron origen a su clasificación.

Por lo expuesto y fundado; se,

R E S U E L V E:

ÚNICO. Se autoriza la ampliación del plazo de reserva de la información, en los términos expuestos en la presente resolución.

Notifíquese instancia requerida y a la Unidad General de Transparencia.

Por unanimidad de votos lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, integrado por el licenciado Mario José Pereira Meléndez, Director General de Asuntos Jurídicos y Presidente del Comité, maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal, y licenciado Adrián González Utusástegui, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; quienes firman con la secretaria del Comité que autoriza.

LICENCIADO MARIO JOSÉ PEREIRA MELÉNDEZ
PRESIDENTE DEL COMITÉ

fundada y motivada, aplicando la prueba de daño y señalando el plazo de reserva, por lo menos con tres meses de anticipación al vencimiento del periodo.”

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=

MAESTRO CHRISTIAN HEBERTO CYMET LÓPEZ SUÁREZ
INTEGRANTE DEL COMITÉ

LICENCIADO ADRIÁN GONZÁLEZ UTUSÁSTEGUI
INTEGRANTE DEL COMITÉ

MAESTRA SELENE GONZÁLEZ MEJÍA
SECRETARIA DEL COMITÉ

"Resolución formalizada por medio de la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL), con fundamento en los artículos tercero y quinto del Acuerdo General de Administración III/2020 del Presidente de la Suprema Corte de Justicia de la Nación, de diecisiete de septiembre de dos mil veinte, en relación con la RESOLUCIÓN adoptada sobre el particular por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación en su Sesión Ordinaria del siete de octubre de dos mil veinte."

NubHAtc0yfpM8gPkptviGR/TH9WNQNlRnVVw0tF+l6k=